Mac OS X Open Directory

Authentication Overview

Session 607

Mac OS X Open Directory

Authentication Overview

David M. O'Rourke
Engineering Manager
daveo@apple.com

Authentication Overview

- Review of current Jaguar feature set
- Cover new features for Panther
  - Local Authentication
  - Open Directory Password Server enhancements
  - Apple's Single Sign-on implementation
- Summary and Wrap up
- Questions and Answers

Jaguar Authentication

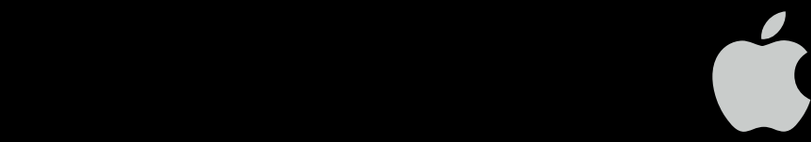
- Jaguar currently supports
  - Crypt
  - Open Directory Password Server
  - Kerberos
  - LDAP Bind
  - Other methods via Directory Service plug-in(s)
- New user attribute “Authentication Authority”
  - Used by Jaguar to determine the best method for authenticating a user

Authentication Authority Matrix

Authentication Authority	Example	Comment
;basic;	;basic; or empty	Crypt-based passwords stored in the user record in the password field
;ApplePasswordServer;	;ApplePasswordServer;[ID][PublicKey][Network Address]	Used to indicate password server based user—no readable password hash

Jaguar Changes

- Entire Operating System was migrated from crypt passwords to API abstractions
  - Login Window
  - Security Framework
  - PAM
  - Directory Service API's
- All Apple software was updated to "not care" how passwords are handled



Open Directory Password Server

- Jaguar Server introduced the Open Directory
- Password Server
- Based on the Open Standard of SASL
- Provides comprehensive network authentication support for a wide array of network protocols

Network Authentication Methods

Authentication Method	Protocol Client
MD5 Digest	Default, Login Window, Clear Text
CRAM-MD5	IMAP and SMTP
NT-Lan Manager	SMB File Sharing
APOP	POP3 Mail Protocol
WebDAV Digest	WebDAV File System
2 Way Random	AFP
DHX (Diffie-Helman Exchange)	AFP, and Mac OS X Setpassword

Example Password Server Authentication

Client accessing network service

Mac OS X Client

Jaguar Server
afp, ftp, imap, smb

Directory Server

Password Server

Example Password Server Authentication

Client contacts network service…

Mac OS X Client

Jaguar Server
afp, ftp, imap, smb

Directory Server

Password Server

Example Password Server Authentication

Server resolves user record…

Mac OS X Client

Jaguar Server
afp, ftp, imap, smb

Directory Server

Password Server

Example Password Server Authentication

Authentication redirects to Password Server…

Mac OS X Client

Jaguar Server
afp, ftp, imap, smb

Directory Server

Password Server

Example Password Server Authentication

Users is granted access—success!!

Mac OS X Client

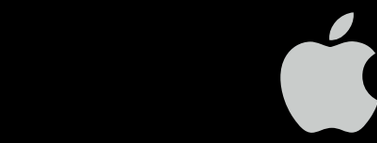
Jaguar Server
afp, ftp, imap, smb

Directory Server

Password Server

Password Server Advantages

- Maintains a single password for all network protocols
  - Allows support for secure legacy network protocols
  - Supports long passwords (511 bytes)
- Enforces password policies for all accounts
- Not subject to “hacking” via download of hashes
- Supports standard security techniques
  - Slows down for successive failures (Panther)
  - Policies to shut down accounts that have been “attacked”
- Uses RSA public-key/private-key to prevent spoofing



Jaguar Kerberos Support

- Jaguar came with full Kerberos support
  - MIT provided Mac OS X Kerberos client
  - Apple support provided configuration documentation
    - http://docs.info.apple.com/article.html?artnum=107153
- Apple Kerberized servers/clients

Jaguar	Jaguar Server
AFP	AFP
Mac OS X Mail	IMAP/SMTP
Login Window	FTP
Telnet	

Jaguar Wrap Up

- Apple expanded the set of choices for authentication with Jaguar
- Abstracted the OS to allow Apple to move quickly in the area of authentication
- Panther is going to introduce even more changes…

Authentication in Panther

Authentication in Panther

Local Authentication

Local Authentication Changes

- Crypt is dead
  - Default local authentication is now stored in a shadow
  - File for all local user accounts
  - Crypt still works—but no tools create crypt users
- Your application should not be relying on
- Crypt passwords
  - Panther will break crypt-based applications
  - This is not an OS bug
- Adopt a password verification abstraction

Password Verification Abstractions

- There are 3 major documented abstractions you can use
  - PAM (pluggable authentication modules)
  - Security Framework
  - Directory Services API's
- If your application is not using one of these API's it will break when running on Panther

Password Verification Abstractions

If your application is not using one of these API's it will break when running on Panther

Authentication Authority Matrix

Authentication Authority	Example	Comment
;basic;	;basic; or empty	Crypt based passwords stored in the user record in the password field
;ApplePasswordServer;	;ApplePasswordServer;[ID][PublicKey][Network Address]	Used to indicate password server based user—no readable password hash
;ShadowHash;	;ShadowHash;	Indicates a user record has a password hash stored in '/var/db/shadow/'

Panther Shadow Hash

- Panther stores all passwords in /var/db/shadow/
  - Secure file system directory
  - Uses Sha-1, supports more than 8 characters
  - System is no longer subject to “hash” download attacks
- Crypt is still supported
  - No administration tools in Panther will create a crypt-based user record
- Panther command line tools updated to use Directory Service API’s to change passwords

Authentication in Panther

Open Directory Password Server Enhancements

Password Server New Features

- New authentication methods for Panther Server
- Secure multi-master replication support
  - Client side fail over
- Global and per-user policies
  - Integrated support for Apple's Kerberos server
- Better performance—less network traffic
- New command line tools to automate policy management

New Authentication Methods

- Password Server has been enhanced to offer new authentication methods to support Panther Server
  - Support for VPN authentication (MS-Chap 2)
  - Support for PDC authentication

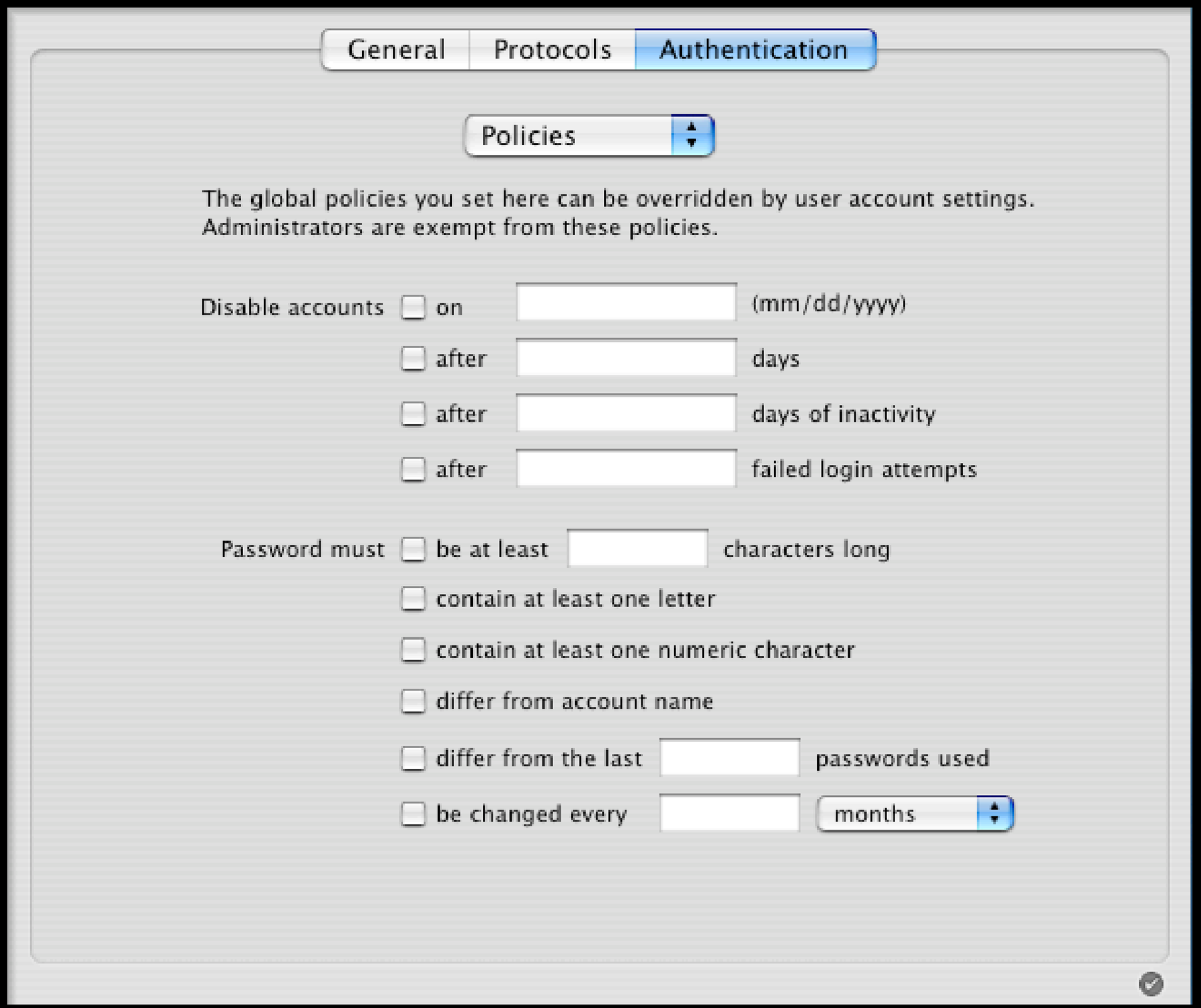
Password Server Authentication Methods

Authentication Method	Jaguar	Panther	Protocol Client
MD5 Digest	✓	✓	Default, Login Window, Clear Text
CRAM-MD5	✓	✓	IMAP and SMTP
NT-Lan Manager	✓	✓	SMB File Sharing
APOP	✓	✓	POP3 Mail Protocol
WebDAV Digest	✓	✓	WebDAV File System
MS Chap2		✓	PPP, PPTP, VPN
2 Way Random	✓		AFP
DHX (Diffe-Helman Exchange)	✓	✓	AFP, and Mac OS X Setpassword

Enhancements to Password Server

- New password policies
  - Global/per-user password policies
    - Allows setting of policy in one place
    - Or for certain users you can override the standard policies
  - New policy features
    - History
    - Character-set requirements
- New tool for policy management—pwpolicy
- Easier to show the new features rather than inventory

Global Policy Screen Shot



Password Policy Screen Shot

Per-user policy settings

Secure Replication

- Password Server leverages public-key/private-key to build a secure system
  - Replication occurs on change or periodically
  - All replicas can accept change password
  - Data is merged between two replicas
- All replication sessions are encrypted end-to-end
  - 128-bit key—RC5 encryption
- Client's replica discovery is quite exhaustive

Client Side Fail Over

- Replica picking is transparent to Directory Server API Client
- Replica discovery is done in parallel—no serial time-outs
- Multi-layered replica discovery
  - Local Cache file
  - Configuration Record in Directory Server
  - Rendezvous
  - Local machine
  - Network address in Authentication Authority
- If a replica is available we will find it!

Rendezvous

- Rendezvous discovery method is secure
  - We’re attempting to resolve the public-key
  - Client will still challenge replica to prove it knows the private key via random number challenge

Integrated Kerberos Support

- Apple will ship an enhanced MIT KDC
- Enhancements allow Password Server and KDC to synchronize password and policy information
- Apple's KDC data leverages Password Server replication
- From a customer's point of view Password Server and KDC are a single system
- Legacy authentication support provided by Password Server provides a gentle migration for customers
- Which brings us to…

Authentication in Panther

Apple’s Single Sign-on Strategy
Why Kerberos is in Apple’s future and yours…

Single Sign-on

- Apple is adopting Kerberos as a network single sign-on approach
- Apple is basing all their Kerberos work on the MIT Kerberos implementation
  - Panther can be configured to work with existing Kerberos deployments
  - Apple is not changing Kerberos
  - Providing configuration tools to make it easier to adopt
- Kerberos is excellent but has suffered from some barriers to adoption

Barriers to Kerberos Adoption

Requires KDC deployment

Directory Server integration

Lack of integrated user account management

Registration of all host/service principals

Command line level configuration of Kerberos clients

No support for legacy network authentication

Panther Server Addresses Barriers to Adoption

✓ Requires KDC deployment	Panther Server will ship with a full KDC—setup by default
✓ Directory Server integration	Directory Service Tools in Panther Server are fully Kerberos aware
✓ Lack of integrated User account management	Panther Server Workgroup Manager automatically creates User principals
✓ Registration of all host/service principals	Panther Server configuration will compose host/service principals
✓ Command line level configuration of Kerberos clients	Panther Desktop will optionally auto configure desktop client for Kerberos
✓ No support for legacy network authentication	Full integration with Password Server means network administrators don't have give up legacy client authentication

Kerberos and Panther

- Kerberos will be fully supported in Panther
- Apple Single Sign-on changes don’t modify Kerberos
  - Apple has provided some automated tools to assist users with configuration
  - Panther Server will be auto configured to support Kerberos if Panther Directory Services are deployed
  - Integration with non-Apple Kerberos systems is no different than any other platform
    - Administrator is responsible for all Kerberos configuration

How Does Panther Auto-Configure Kerberos?

- Login Window has been modified to “key” off of a Kerberos Authentication Authority in the user record
  - If Panther “sees” a Kerberos Authentication Authority in a user record Kerberos client configuration data will be used from corresponding directory
  - If there is no configuration data in the directory no action is taken
- Sites can add auto-configuration data to legacy deployments or leave it out if they prefer manual configuration

Customers Can Choose

- Customer can choose to deploy Apple's services
  - Kerberos will be easier than ever with Panther Desktop and Server
  - Many barriers to Kerberos deployment are addressed in Panther Desktop and Server
- Customers can configure Panther to work with existing Kerberos deployments
  - No different than other Kerberos platforms

Authentication Long Term

- Apple is investing heavily in Kerberos
  - Aggressively migrating all networking products to be Kerberos-based
  - Apple will ship the MIT KDC
  - Apple already ships the MIT Kerberos client
  - Session #108 is a must attend for any network service developers
- All Kerberos all the time is in Apple's future and yours
- Plan today for the changes you know are coming…

Wrap Up

Authentication Overview

- Jaguar introduced new authentication support
- Panther has changes in 3 important areas
  - Local Authentication
  - Open Directory Password Server enhancements
  - Apple's Single Sign-on implementation

Password History and Future

Crypt

Mac OS 10.0

Crypt
LDAP Bind
DS API

Mac OS 10.1

Crypt
LDAP Bind
Kerberos
DS API
Password Server
PAM
Security Framework

Mac OS 10.2

LDAP Bind
Kerberos
DS API
Password Server + Replication
PAM
Security Framework

Panther

Roadmap

101 Security: Architectural Overview	The Marina Mon, 5:00pm
108 Kerberos in Mac OS X	The Mission Thu, 9:00am
604 Mac OS X Server Overview	The Mission Tue, 2:00pm
606 Mac OS X Server in Depth	The Marina Tue, 3:30pm
610 Directory Services	The Mission Wed, 10:30am
611 Managed Desktop Technologies	Nob Hill Wed, 2:00pm
622 Network Security Best Practices	Nob Hill Fri, 10:30am

Who to Contact

David M. O'Rourke
Engineering Manager
daveo@apple.com

Skip Levens
Server Technology Evangelist
slevens@apple.com

http://developer.apple.com/wwdc2003/urls.html

For More Information

Reference Library

Documentation, Open Source, References

Directory Services API Documentation

http://developer.apple.com/techpubs/macosx/Networking/Open_Directory/index.html

http://developer.apple.com/techpubs/macosx/Networking/Open_Dir_Plugin/index.html

Darwin Open Directory

http://developer.apple.com/darwin/projects/opendirectory/

Open Directory SDK

ftp://ftp.apple.com/developer/Development_Kits/DirectoryServicesSDKv1.0.dmg.bin

Reference Library

Documentation, Open Source, References

Mac OS X Server Documentation

http://www.apple.com/server/macosx/resources.html#g

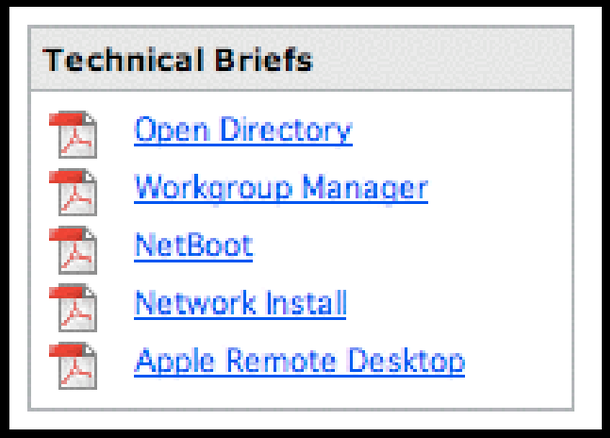
http://www.apple.com/server/desktop_management.html

Mac OS X LDAP schema

Open LDAP Configuration files

Mac OS X Security APIs

http://developer.apple.com/darwin/projects/cdsa/



Reference Library

Documentation, Open Source, References

Open LDAP
http://www.openldap.org/

SASL
http://asg.web.cmu.edu/sasl/

PAM
http://www.kernel.org/pub/linux/libs/pam/

Kerberos
http://web.mit.edu/kerberos/www/

Who to Contact

Andreas Wendker
Manager, WebObjects Engineering
webobjects@apple.com

Bob Fraser
Senior Product Manager, WebObjects and Java
webobjects@apple.com

Katherine Wenc
Manager, Technical Publications
webobjects@apple.com

Enterprise-Level WebObjects Support And Consulting
AppleCare Enterprise Services
services@apple.com
(800) 630 2775

http://developer.apple.com/wwdc2003/urls.html

Reference Library

Resources

Product Information
http://www.apple.com/webobjects

Developer Support
http://developer.apple.com/webobjects

Enterprise-Level WebObjects Support And Consulting
http://www.apple.com/services/technicalsupport
http://www.apple.com/services/consulting

Mailing List

WebObjects Announcements
webobjects-announce@apple.com

Q&A

David M. O'Rourke
Engineering Manager
daveo@apple.com

http://developer.apple.com/wwdc2003/urls.html

WWDC 2003

Worldwide Developers Conference